جنگ ریاضی دانشجو، ۱۳۶۹،۶، ۳۸-۶۳

ایان بلیک

کدها و طرحها●

ترجمهٔ شاهین آجودانی نمینی

طرحهای ترکیبیاتی که با الگوهایی از زیر مجموعه‌های یك مجموعه ساخته می‌شوند، درهایی به سوی دستیابی به کدهای سودمند می‌گشایند.

نظریهٔ جبری کدگذاری بیش‌از بیست و پنج‌سال قدمت‌دارد، پیدایش این‌نظریه مرهون قضیهٔ معروف شنون [۱] دربارهٔ کدگذاری‌نویزی است که خطای عملکرد یك کانال گسسته را تخمین می‌زند، بی آنکه اشاره‌ای به‌نحوهٔ دستیابی به‌این‌خطا کند. اززمان اثبات آن تاکنون، ارتباط متقابل میان نظریهٔ کدگذاری ودیگر شاخه‌های ریاضیات، به‌خصوص نظریهٔ گروهها و آنالیز ترکیبیاتی، مداوماً توسعه یافته است. نتیجهٔ این تأثیر متقابل، مبحث زیبایی است که نتایج و روشهایی فراهم‌می‌سازد که می‌توانند درمسائلی بااهمیت زیادکاربردی مفیدباشند.

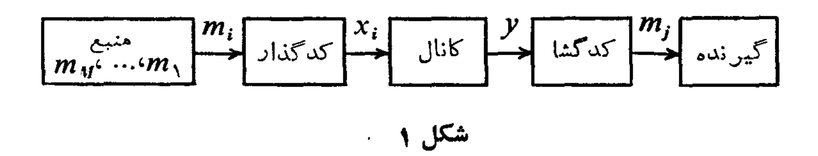
دراین‌مقاله درنظر دارم‌ارتباط میان‌کدگذاری و برخی‌ازطرحهای‌ترکیبیاتی‌را بررسی کنم. نخست برخی‌از مفاهیم‌اساسی‌نظریهٔ‌کدگذاری را معرفی خواهم‌کرد و تعدادی‌ازکدهای موردنیازرا خواهم‌ساخت. ازآنجا که‌کدهای دودویی مورد توجه‌خاص‌ماهستند، بسیاری از مفاهیم‌راتنها دراین‌حالت شرح خواهم‌داد. شمارش‌وزن کدها، که‌فی‌نفسه مبحث جالبی‌است، دریافتن‌طرحهاازمیان‌کدها نیز سودمندند؛ بنابراین برخی‌ازنتایج مربوط به آن‌بیان‌شده‌است. سپس برخی‌ازطرحهای‌ترکیبیاتی راکه ازدیدگاه کدگذاری مورد توجه‌اند شرح‌می‌دهیم، و برخی‌ازخواص آنها رابیان‌می‌کنیم. درادامه، نتایج این‌بخشهارا برای‌اثبات سلسله قضایای منسوب به آسموس[1] و ماتسون[2] به‌کارمی‌بریم. این‌قضایا نشان‌می‌دهندکه چگونه می‌توان از کدهای "خوب" طرح‌ساخت. دربخش نهایی‌مقاله سعی‌داشته‌ام‌تعمیمها و پیشرفتهای اخیراین

● Blake, Ian, "Codes and designs," *Mathematics Magazine*, **52**(1979) 81-95.

1. Assmus 2. Mattson

مباحث را نشان دهم، ومطالبی نیز درمورد منابع ومقالات دراین‌زمینه آورده‌ام.

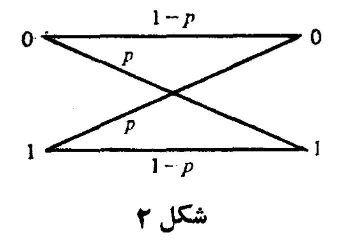
اهداف این‌مقاله تاحدودی بلندپروازانه است، بنابراین ناچار بودم‌که تصمیم بگیرم که‌چه چیزهایی اثبات وچه‌چیزهایی تنها بیان‌شود. هدف‌من آشنا ساختن‌خواننده باخطوط کلی این‌مبحث وروشهای نظریهٔ کدگذاری است، بی‌آنکه بر روی هیچ یك‌از این‌مباحث بیش‌ازحد تأکیدشود. اخیراً دومقاله‌منتشر شده‌است که نظریهٔ کدگذاری و آنالیز ترکیبیاتی رامرورمی‌کنند [۲ و ۳]؛ این‌مقالات هردوعمیقتر وجامعتر ازاین مقاله‌اند، وخواننده‌ای که این‌مقاله را باب طبع‌خودبیابد، حتماً باید آن‌دومقاله راهم بخواند. به‌ویژه مقالهٔ آسموس وماتسون [۲] در تهیهٔ این مقاله، که درواقع مروری‌بر کار آنهاست، مفید بوده‌است.



شکل ۱

کدها

به‌منظوریافتن انگیزه‌ای برای‌مطالعهٔ کدگذاری، مدل‌ساده‌ای ازیك شبکهٔ ارتباطی راکه در شکل ۱ نشان‌داده‌شده‌است، درنظرمی‌گیریم. دراین‌مدل ازمیان M پیام‌ممکن $m_1, \dots, m_M$، پیام m_i برای‌انتقال برگزیده می‌شود. کدگذار[1] این پیام رابه‌یك رشتهٔ دودویی به‌طول N، $x_i=(x_{i_1}, \dots, x_{i_N})$، که در آن $x_{i_j}\in\{0,1\}$، تبدیل‌می‌کند. این رشته کدواژهٔ[2] پیام m_i نامیده‌می‌شود. درهرواحد زمانی کانال یکی از این نمادهای دودویی را می‌پذیرد و آن را یا به‌طورصحیح وبااحتمال $1-p$ ویابه‌صورت خطا وبا احتمال p، به‌گیرنده انتقال می‌دهد.



شکل ۲

چنین کانالی یك کانال دودویی متقارن (BSC) نامیده می‌شود و در شکل ۲ نشان داده شده است. کدگشا[3] که‌فهرستی‌ازتمام‌کدواژه‌های ممکن x_i، M، $i=1,2,\dots,M$، رادراختیاردارد، پس‌ازدریافت N رقم y باتوجه به‌آزمون‌کمترین احتمال خطاتشخیص می‌دهدکه‌کدام پیام مخابره شده است. اگر پیام m_i فرستاده شده باشد، ولی کدگشا تشخیص دهدکه پیام m_j،

1. coder 2. codeword 3. decoder

$j \neq i$ ، مخابره‌شده‌است، آنگاه یك‌خطای کدگشایی صورت گرفته‌است واحتمال‌وقوع چنین خطایی p_e است. ظرفیت BSC به صورت $C = 1 + p\log_2 p + (1-p)\log_2(1-p)$ ونرخ‌کد به‌صورت $R = (\log_2 M)/N$ تعریف می‌شود. قضیهٔ‌اساسی شنون می‌گوید که به ازای هر $\delta > 0$، اگر $R < C$، آنگاه‌برای N به‌اندازهٔ‌کافی بزرگ کدی به‌طول N با نرخ $R' > R$ وجوددارد به‌طوری‌که $p_e < \delta$. بنابراین می‌توان درمکالمات احتمال‌خطارا به‌هر اندازهٔ دلخواه‌کوچك‌کرد ونرخ راثابت نگاه‌داشت، مشروط به‌آنکه طول‌کد به‌اندازهٔ کافی بزرگ باشد. البته‌این‌کار به‌قیمت‌افزایش پیچیدگی سیستم، وتأخیردراعمال‌کدگذاری وکد گشایی تمام می‌شود.

اثبات این‌قضیهٔ جالب‌توجه ازطریق استدلالهای کدگذاری تصادفی‌صورت‌می‌گیرد. به‌طورخلاصه، ازبین 2^N کدواژهٔ ممکن، M تا به‌طورتصادفی وباتوزیع‌احتمال معینی‌انتخاب می‌شوند. احتمال بروزخطای حاصل به‌مجموعهٔ همهٔ‌کدهای ممکن‌بااندازهٔ M محدود می‌شود، وباید دست‌کم یك‌کد وجودداشته باشدکه‌این‌کران میانگین را برآورده سازد. البته، چنین فرایندهای کدگذاری تصادفی‌ای برای‌اهداف عملی مناسب‌نیستند وروشهایی برای‌کدسازی موردبررسی قرارگرفته‌اند که ازنظر کارایی برآورندهٔ کران مورد نظر باشند. نتیجهٔ این مطالعات، پیدایش نظریهٔ جبری‌کدگذاری است.

ماکارخود را باتعریف ساختارها ورهیافتهای بنیادی به‌نظریهٔ‌کدگذاری‌آغازمی‌کنیم. میزان توجهی‌که به‌رهیافتهای دیگرشده درجات مختلفی‌داشته‌است، امااین‌رهیافتها آنقدرها پیشرفت نکرده‌اندکه به‌طورگسترده مورد مطالعه قرارگیرند. ساختاری بنیادی‌که اساساً کاپهٔ کارهای تحقیقاتی درزمینهٔ‌کدگذاری حول‌وحوش آن‌صورت می‌گیرد، فضای برداری با بعد متناهی روی‌یك میدان‌متناهی‌است. اگر q توانی‌ازیك عدداول باشدمیدان متناهی q عنصری را، که در حد یکریختی یکتاست، با F_q نشان می‌دهیم. گهگاه به خواصی ازاین میدان، که ممکن‌است چندان مشهور نیزنباشند، نیازخواهیم داشت، امابه‌جای آنکه اکنون به‌شرح این خواص بپردازیم، آنهارادرمواقع لزوم بیان خواهیم‌کرد. فرض‌کنید F_q^n فضای برداری n بعدی‌روی F_q باشد. F_q^n نیز در حد یکریختی یکتاست وآن‌را به‌صورت‌مجموعهٔ n تاییهای روی F_q درنظرمی‌گیریم.

وزن (همینگ) عنصر $x \in F_q^n$، یعنی $w(x)$، عبارت‌است‌از تعداد مختصات ناصفر x، و **فاصلهٔ** (همینگ) دوعنصر x و y از F_q^n، یعنی $d(x,y)$، به‌عنوان تعدادمختصاتی‌که xوy درآنها برابر نیستند تعریف‌می‌شود، وبنابراین $d(x,y) = w(x-y)$. یك زیرمجموعهٔ C از F_q^n رایك **کد** (n,M,d,q) می‌نامیم هرگاه $M = |C|$، که‌درآن $|C|$ تعداد عناصر C است، و $d = \min\{|d(x,y)| \, x,y \in C, x \neq y\}$. اگر C زیر فضایی k ـ بعدی از F_q^n باشد، آن‌را یك **کدخطی** یایك **کد** (n,k,d,q) **خطی** می‌نامیم.معمولاً q ثابت و d مجهول است یا اینکه در آن مبحث خاص به d نیازی نیست. در این حالات C را به طور ساده یك‌کد (n,k) خطی می‌نامیم. به سادگی دیده می‌شودکه برای هرکد خطی، $d = \min\{w(x) | x \in C, x \neq 0\}$.

مسئلهٔ‌کدگذاری ازاین قراراست: چنانچه n و M (وq) داده شده‌باشد، کدواژه‌ها را

چنان اختیار کنید که d بیشینه شود. به‌عکس، چنانچه n و d داده‌شده باشد. مسئله بیشینه‌ساختن M خواهد بود. اگر $e=[(d-۱)/۲]$ (که $[x]$ جزءصحیح x را نشان می‌دهد)، کره به شعاع e حول نقطهٔ $x\in F_q^n$ را به‌صورت $S_e(x)=\{y\in F_q^n|d(x,y)\leqslant e\}$ تعریف کنید. حال، واضح است که $|S_e(x)|=\sum_{j=۰}^{e}\binom{n}{j}(q-۱)^j$ ، زیرا دقیقاً $(q-۱)^j$ عضو در F_q^n وجود دارد که با x در j مختص مفروض اختلاف داشته باشد، و $\binom{n}{j}$ روش برای انتخاب این j مختص وجود دارد. درمسائل گزینش کدواژه‌ها که هم اکنون مطرح شد، مجموعهٔ همهٔ چنین کره‌هایی حول کدواژه‌ها، دو به‌دو اشتراك تهی دارند و به سادگی دیده می‌شود که برای یك کد (n,M,d,q)، $M|S_e(x)|\leqslant q^n$، که در آن $e=[(d-۱)/۲]$. این نتیجه اغلب **کره‌چینی**[1] یا **کران همینگ-رائو** [2] نامیده می‌شود، و هر کدی که کران فوق را با علامت تساوی بر آورده سازد یك کد **کامل** نامیده می‌شود. توجه کنید که برای یك کد کامل d لزوماً فرد است.

از آنجا که برای هر کد کامل با فاصلهٔ مینیمم d، کره‌های به‌شعاع $e=[(d-۱)/۲]$ حول کد واژه‌ها همگی غیر متقاطع‌اند، می‌توانیم الگوریتم کدگشایی را برحسب مینیمم فاصله به‌کار بریم. اگر n تایی دریافتی $y\in F_q^n$ در کرهٔ به‌شعاع e و حول $c\in C$ قرارگیرد، y را با c کدگشایی می‌کنیم. اگر در انتقال کمتر از e خطا رخ داده باشد، کدگشایی صحیح خواهد بود. اگر در انتقال بیش از e خطا رخ داده باشد، یا y به یك واژهٔ نادرست کدگشایی خواهد شد (y در کرهٔ به‌شعاع e حول کدواژه‌ای متفاوت با کدواژهٔ ارسال‌شده قرار خواهد گرفت) یا اینکه y در هیچ شعاع eای حول یك کدواژه قرار نمی‌گیرد که در این صورت باید استراتژی دیگری را، مثل تقاضای ارسال مجدد این کدواژه، پیش بگیریم. از این ملاحظات سرشت کره چینی در مسئلهٔ کدگذاری دیده می‌شود. البته درعمل تکنیکهای دیگری نیز به‌کار می‌روند که در کدگشایی مؤثرند و در اینجا بررسی نخواهند شد.

برای حصول موفقیت بیشتر در شرح کدهای خطی، نخست توجه می‌کنیم که اگر C یك کد خطی (n,k) باشد، کد را می‌توان به‌صورت فضای سطری یك ماتریس $k\times n$ روی F_q مانند G در نظر گرفت و هر مجموعه از k کدواژهٔ مستقل خطی C را می‌توان به‌عنوان سطرهای G انتخاب کرد. ماتریس G ، یعنی **ماتریس مولد** کد ، را می‌توان با تحویل سطری به شکل استاندهٔ $G'=[I_k:A]$ درآورد که در آن A یك ماتریس $k\times(n-k)$ است. اگر عمل کدگذاری را به‌صورت ضرب ماتریسی $c=iG'$ در نظر بگیریم که در آن i یك رشتهٔ اطلاعاتی k تایی روی F_q، و c کدواژهٔ نظیر آن است، آنگاه نخستین k مختص c، i را تشکیل می‌دهند ، و $(n-k)$ مختص باقیمانده برای آزمون زوجیت[3] این k مختص اول به‌کار می‌روند. کدی که خانه‌های اطلاعاتی آن صریحاً معلوم باشند، سازمان یافته (سیستماتیك) نامیده می‌شود.

اگر C کدی خطی باشد، می‌توان مفهوم مفید **کد** (یا فضای) **دوگان** را به‌طور طبیعی با

1. sphere packing 2. Rao 3. Parity

$$C' = \{y \in F_q^n | (x,y) = \sum_{i=1}^{n} x_i y_i = 0, \forall x \in C\}$$

تعریف کرد که در آن حاصلضرب داخلی در F_q محاسبه شده است. کد دوگان خود یك کد خطی است (مفهوم دوگان برای یك کد غیرخطی به وضوح داده نشده است). برای یك فضای برداری حقیقی، چنانچه دوگان یك زیرفضا به طریق مشابه تعریف شود، داریم $C \cap C' = \{0\}$ و $\dim C + \dim C' = n$. اما برای F_q^n تنها رابطهٔ $\dim C + \dim C' = n$ درست است. برای مثال اگر $C \subset F_2^4$ عبارت باشد از

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

آنگاه $C = C'$؛ این خاصیت برای کسانی که به برداشت هندسی از فضاهای حقیقی خو گرفته‌اند، عجیب به شمار می‌آید.

یك ماتریس مولد H برای دوگان C' از کد (n,k) خطی C، ماتریسی $n \times (n-k)$ ای است که فضای سطری آن C' است و ماتریس **آزمون زوجیت** C نامیده می‌شود. بنا به تعریف، این ماتریس در معادلهٔ $GH^T = 0$ صدق می‌کند. اگر G به شکل استاندهٔ $[I_k : A]$ باشد، آنگاه $H = [-A^T : I_{n-k}]$. یك خاصیت مهم ماتریس آزمون زوجیت که باید آن را به خاطر بسپاریم از این قرار است: اگر همهٔ عناصر کدواژهٔ $x \in C$ صفر نباشند، آنگاه $xH^T = 0$، اما از آنجا که xH^T ترکیبی خطی از ستونهای H است، ستونهایی از H که با درایه‌های ناصفر x متناظرند، وابستهٔ خطی‌اند. درنتیجه، اگر هیچ $(d-1)$ ستونی از H وابستهٔ خطی نباشند، فاصلهٔ مینیمم C دست کم برابر d است. از این استدلال کرانی نیز برای کدها به دست می‌آید. از آنجا که رتبهٔ H حداکثر $n-k$ است، در بهترین حالت هر مجموعه از $(n-k)$ ستون مستقل است، و بنا براین $d-1 \leqslant n-k$ یا $d \leqslant n-k+1$ که **کران سینگلتون**[1] کدگذاری نامیده می‌شود. هر کدی که کران فوق را با علامت تساوی بر آورده سازد، یك **کد بهینه** نام دارد. توجه کنید که کاربرد هنرمندانهٔ کد دوگان به کسب اطلاعاتی درمورد خود کد انجامید.

مثالی از این ایده‌ها می‌تواند مفید باشد. کد $(7,4)$ خطی دودویی C را با ماتریس آزمون زوجیت

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \qquad (1)$$

---

1. Singleton bound

در نظر بگیرید وملاحظه کنیدکه هر سه‌تایی ناصفر به‌عنوان ستونی‌از H ظاهر می‌شود. از آنجا که هر دو ستون مستقل خطی‌اند، فاصله مینیمم C برابر ۳ است. روش بهتری برای بررسی این‌کد (که اصلا ساختهٔ همینگ است [۴]) آن است که هر کدواژه را به صورت $(p_1, p_2, i_1, p_3, i_2, i_3, i_4)$ در نظر بگیریم که i_4, i_3, i_2, i_1 رقمهای حاوی اطلاعات، و p_1، p_2 و p_3 رقمهای آزمون زوجیت‌اند. این ارقام در معادلات F_2

$$p_1 + i_1 + i_2 + i_4 = 0$$

$$p_2 + i_1 + i_3 + i_4 = 0$$

$$p_3 + i_2 + i_3 + i_4 = 0$$

صدق می‌کنند. برای مراجعات بعدی، توجه کنید که کدواژه‌های C عبارت‌اند

۰۰۰ ۰۰۰۰	۱۱۱ ۰۰۰۰	۱۱۰ ۰۱۱۰	۰۱۱ ۰۰۱۱
۱۱۰ ۱۰۰۱	۱۰۰ ۰۰۱۱	۱۰۱ ۱۰۱۰	۱۰۱ ۰۱۰۱
۰۱۰ ۱۰۱۰	۰۱۰ ۰۱۰۱	۰۱۱ ۱۱۰۰	۰۰۱ ۰۱۱۰
۱۰۰ ۱۱۰۰	۰۰۱ ۱۰۰۱	۰۰۰ ۱۱۱۱	۱۱۱ ۱۱۱۱

از آنجا که

$$M|S_1(x)| = 2^4\left(\sum_{i=0}^{1} \binom{7}{i}\right) = 2^7 = |F_2^7|$$

کدکامل است و کد (۷,۴) دودویی همینگ نامیده‌می‌شود.

تعمیم این‌مثال‌وشرح ردهٔ‌همهٔ کدهای‌همینگ، چندان‌مشکل نیست و اکنون به آن‌می‌پردازیم. ماتریس $k \times n$ آزمون زوجیت H راروی F_q طوری می‌سازیم که ستونهایش همهٔ $n = (q^m - 1)/(q - 1)$، mتاییهایی از F_q باشندکه هیچ دوتایشان مضرب اسکالری از دیگری‌نیستند. کد C باماتریس آزمون‌زوجیت H، طولی برابر $n = (q^m - 1)/(q - 1)$، بعدی برابر $n - m$ وفاصله‌ای برابر ۳ دارد، وبازهم کامل‌است، زیرا

$$M|S_1(x)| = q^{n-m}\left(\sum_{i=0}^{1} \binom{n}{i}(q-1)^i\right) = q^n = |F_q^n|$$

اخیراً ثابت‌شده‌است [۵و۶] که‌تنها دو کدخطی‌کامل‌دیگروجوددارد، که‌این‌دورا نیز تاپایان این بخش‌معرفی‌خواهیم‌کرد، ونیز در کدکامل دیگری غیرخطی‌است، ودقیقاً همان‌پارامترهای (طول، فاصله، اندازه) کدهای همینگ رادارد.

وضعیت مختصات یك‌کد خطی C به‌طول n، اغلب با اعضای $\{0, 1, \ldots, n-1\}$ شماره‌گذاری می‌شود. عملی‌که به‌نوبهٔ خودمفید خواهدبود توسیع C است‌که آن را با C_e

نمایش می‌دهیم و به‌این صورت انجام می‌گیرد که یك رقم آزمون زوجیت را طوری اضافه می‌کنیم که‌مجموع همهٔ‌مختصات صفر شود. به‌عنوان نتیجه‌ای‌ازمحاسباتی که توسط گروههای خطی‌کسری روی‌کدها انجام‌شده است، مختص‌اضافی را با ∞ برچسب می‌زنیم. اگر C یك کد (n,k) باشد، آنگاه C_e یك‌کد $(n+1,k)$ است و اگر H ماتریس آزمون زوجیت C باشد، ماتریس زیرماتریس آزمون زوجیت C_e خواهد بود

$$H'=\left[\begin{array}{cccccccc|c} 0 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & n-1 & \infty \\ \hline & & & & & & & & 0 \\ & & & & & & & & 0 \\ & & & H & & & & & \vdots \\ & & & & & & & & 0 \\ \hline 1 & 1 & \cdot & \cdot & \cdot & \cdot & 1 & 1 & 1 \end{array}\right]$$

روی میدانهای غیردودویی گاهی‌اوقات مختص‌اضافه شده بامضربی ازمجموع دیگرمختصات پرمی‌شود تا شرایط معینی درمورد دوگان کدتوسعه یافته برقرار شود. ازتوسعهٔ‌کد (۷,۴) همینگ، کدی به‌طول ۸ حاصل می‌شود. درنتیجهٔ این توسعه، ۷ برداری که وزنشان در C برابر۳ است، به‌بردارهای به‌وزن ۴ در C_e تبدیل‌می‌شوند، و به بردارهای به‌وزن ۴ در C یك‌مختص صفر اضافه می‌شود. بنابراین C_e ۱۴ بردار به‌وزن ۴، یك بردار به‌وزن ۰، و یك بردار به‌وزن ۸ دارد، وکدی (۸,۴) بافاصلهٔ ۴ است.

مفهوم‌مهم دیگری که به‌آن می‌پردازیم، کد دوری‌است. توجه‌کنیدکه باتعویض‌ترتیب ستونها، ماتریس آزمون‌زوجیت H در(۱) رامی‌توان به‌صورت

$$H'=\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

نوشت، و به‌این‌ترتیب هم‌در C وهم‌دردوگانش C' انتقال دوری‌هر کدواژه بازهم‌یك‌کدواژه است؛ (یــك انتقال دوری از $(c_0,c_1,\dots,c_{n-1})$ به‌صورت $(c_{n-1},c_0,\dots,c_{n-3},c_{n-2})$ تعریف می‌شود). یك کددوری را به‌عنوان کدی خطی‌تعریف‌می‌کنیم که درآن انتقال‌دوری‌هر کدواژه بازهم یك کدواژه باشد؛ به عبارت دیگریك‌کد دوری تحت‌اثر جایگشتهای دوری روی مختصات پایاست. این کدها به طور گسترده‌ای مورد مطالعه قرار گرفته‌اند و اغلب کدهای جالب، کدهای‌دوری ویاگسترش یافته‌های‌آنها هستند.

درمطالعهٔ‌کدهای دوری استفاده ازیك نمادگذاری چند جمله‌ای مفیدخواهد بود: به‌هر کد واژهٔ $c=(c_0,c_1,\dots,c_{n-1})$، یك چند جمله‌ای $c(x)=c_0+c_1x+\dots+c_{n-1}x^{n-1}$ نظیرمی‌کنیم. یك‌انتقال دوری این‌کد واژه با چند جمله‌ای $xc(x)$ به‌پیمانهٔ x^n-1 متناظر است. یك‌کددوری‌متناظر باایده‌آلی‌درحلقهٔ چندجمله‌ایهای $F_q[x]/(x^n-1)$ است.درچنین

حلقه‌ای هر ایده‌آل یك ایده‌آل اصلی، ومولد $g(x)$ آن لزوماً مقسوم علیهی از $x^n - ۱$ است. اگر بعد زیر فضای دوری k باشد، آنگاه درجهٔ چندجمله‌ای مولدش، یعنی $g(x)$، برابر $n-k$ است. بنابراین کد C را می‌توان با ایده‌آل چندجمله‌ای

$$C = \{a(x)g(x) | \deg(a(x)) \leqslant k - ۱, a(x) \in F_q[x]\}$$

توصیف کرد. اگر $x^n - ۱$ تعداد s عامل تحویل ناپذیر روی F_q داشته باشد، آنگاه دقیقاً ۲^s کد دوری به‌طول n روی F_q وجود دارد، زیرا هر مقسوم علیه $x^n - ۱$ یك کد دوری تولید می کند.

حال به‌مرور نتایجی در باب چند جمله‌ایهای روی میدانهای متناهی می‌پردازیم. گروه ضربی F_q^* حاصل از F_q دوری‌است[۱] وهر مولدش یك **عنصر اولیه** نامیده می‌شود. هرمیدان متناهی دست‌کم یك، ودرواقع $\phi(q-۱)$، عنصر اولیه‌دارد که در آن ϕ تابع نشانگر اویلر است. یك **چند جمله‌ای تحویل ناپذیر** روی F_q چندجمله‌ایی‌است که‌نتوان آن‌را به‌صورت حاصلضرب دوچند جمله‌ای بادرجهٔ کوچکتر نوشت. هرچند جمله‌ای تحویل ناپذیر ازدرجهٔ k روی F_q همواره $x^{q^k} - x$ را عاد می‌کند و این چندجمله‌ای به حاصلضرب همهٔ چند جمله‌ایهای تحویل ناپذیری که درجه‌شان k را عاد می‌کند، تجزیه می‌شود. چند جمله‌ای تحویل‌ناپذیر $f(x)$ روی F_q را **اولیه** می‌نامیم اگر $f(x) | x^{q^k-۱} - ۱$، ولی به ازای هر $s < q^k - ۱$، $f(x) \not| x^s - ۱$. اگر β عنصری از توسیع F_{q^k} از F_q باشد، چندجمله‌ای تکین (ضریب بزرگترین توان x یك است) و از کوچکترین درجهٔ ممکن $m_\beta(x)$ را که β یکی ازریشه‌هایش است، چند جمله‌ای می‌نیمال β روی F_q می‌نامیم. به‌ازای هرچند جمله‌ای $f(x) \in F_q[x]$ داریم $f(x^q) = (f(x))^q$، وبنابراین اگر β ریشه‌ای‌از $f(x)$ باشد، β^q، $\beta^{q^۲}$، . . .، نیز چنین خواهند بود و **مزدوجهای** β نامیده می‌شوند. اگر $K = \{\beta, \beta^q, \ldots, \beta^{q^{s-۱}}\}$، که در آن $\beta^{q^s} = \beta$ وبه‌ازای‌هر $۰ < i < s$، $\beta^{q^i} \neq \beta$، آنگاه $m_\beta(x) = \prod_{i=۰}^{s-۱}(x - \beta^{q^i})$، و از آنجا که $m_\beta(x) | x^{q^k} - x$، نتیجه می‌گیریم که s عدد k را عاد می‌کند. هر چند جمله‌ای تکین اولیه از درجهٔ k روی F_q، چند جمله‌ای می‌نیمال عنصر اولیه‌ای از F_{q^k} است.

همانطورکه دیدیم، کد دودویی (۷,۴) همینگ را همواره می‌توان به یك کد دوری تبدیل کرد. درحالت کلی اگر α عنصراولیه‌ای از $F_۲^m$ باشد، چند جمله‌ای مولدکد همینگ به‌طول $۲^m - ۱$ و بعد $۲^m - m - ۱$، یعنی $m_\alpha(x)$، یك چند جمله‌ای اولیه است. برای

---

۱. مقصود ازگروه ضربی F_q^*، گروه $(F_q - \{۰\}, .)$ است.ـم.

کدهای همینگ روی F_q ، اگر α عنصر اولیه‌ای از F_{q^m} باشد، چند جمله‌ای مولد کد $((q^m-1)/(q-1)\ ,(q^m-1)/(q-1)-m)$ همینگ، چند جمله‌ای مینیمال عنصر α^{q-1} است، مشروط بر آنکه $(q-1)$ و m نسبت به‌هم اول باشند [۷].

اگر $g(x)$ چند جمله‌ای مولد یك کد دوری (n,k) مانند C باشد و

$$g(x)h(x)=x^n-1$$

به سادگی دیده می‌شود که C' نیز دوری و چند جمله‌ای مولدش $x^{n-k}h(1/x)$ است.

در بخشهای بعد به‌ردهٔ دیگری از کدها، یعنی کدهای ماندهٔ درجهٔ دوم، نیاز داریم. فرض کنید n یك عدد اول فرد، و α یك ریشهٔ nام واحد دریك توسیع از F_q باشد. فرض کنید R مجموعهٔ مانده‌های درجهٔ دوم در F_n، یعنی $R=\{x\in F_n|\exists a:\ a^2=x\ ,\ x\neq 0\}$، و $\bar{R}$ مجموعهٔ عناصر ناصفر F_n-R باشد. چند جمله‌ایهای

$$g_1(x)=\prod_{r\in R}(x-\alpha^r) \text{ و } g_2(x)=\prod_{r\in \bar{R}}(x-\alpha^r)$$

را درنظرمی‌گیریم‌وفرض‌می‌کنیم (پیمانهٔ n) $q^{(n-2)/2}\equiv 1$، که ایجاب می‌کند q یك‌ماندهٔ درجهٔ دوم در F_n باشد. درحالت دودویی‌کافی است‌که (پیمانهٔ ۸) $n\equiv\pm 1$. از آنجا که حاصلضرب‌دومانده بازهم یك‌مانده است، $qR=R$ ومشابهاً $q\bar{R}=\bar{R}$. بنابراین مزدوجهای هر ریشهٔ $g_1(x)$ بازهم ریشه‌ای از آن‌اند و $g_1(x)$ یك‌چندجمله‌ای روی F_q است و وضعیت مشابهی درمورد $g_2(x)$ نیز برقرار است. کدهای تولید شده توسط $g_1(x)$ و $g_2(x)$ را کدهای ماندهٔ درجهٔ دوم به‌طول n وبعد $(n+1)/2$ می‌نامند.

به‌ویژه ما به دوکد ماندهٔ درجهٔ دوم توجه داریم. پیش از هرچیز، توجه‌کنید‌که $x^n-1=(x-1)g_1(x)g_2(x)$ و به‌ازای $i=1,2$، $g_i(x)|x^n-1$. نخستین کدی که مورد توجه ماست، کدی دودویی است به‌طول ۲۳ باچند جمله‌ای مولد

$$g_1(x)=1+x+x^5+x^6+x^7+x^9+x^{11}$$

یا

$$g_2(x)=1+x^2+x^4+x^5+x^6+x^{10}+x^{11}$$

و این چند جمله‌ایها روی F_2 تحویل ناپذیرند. می‌توان نشان دادکه فاصلهٔ مینیمم کد دوری (۲۳،۱۲)ای‌که توسط هریك از این چند جمله‌ایها تولید می‌شود، برابر ۷ است واز آنجا که $|S_3(x)|=\sum_{i=0}^{3}\binom{23}{i}=2^{11}$ و $M|S_3(x)|=2^{12}.2^{11}=2^{23}=|F_2^{23}|$، کدکامل است.

کد دیگری که بدآن‌علاقه‌مندیم، کدی به‌طول $n=11$ روی $F_3=\{0,1,-1\}$ است. چند جمله‌ایهای $g_1(x)$ و $g_2(x)$ عبارت‌اند از

$$g_2(x)=x^5+x^4-x^3+x^2-1 \quad \text{و} \quad g_1(x)=x^5-x^3+x^2-x-1$$

وهریك از این چند جمله‌ایها یك‌کد (۱۱،۶) بافاصلهٔ $d=5$ تولید می‌کنند. از آنجا که

$\sum_{i=0}^{۲}\binom{۱۱}{i}۲^i=۳^۵$ و $|S_۲(x)|=|F_۳^{۱۱}|=۳^{۱۱}=۳^۶.۳^۵=M|S_۲(x)|$، ایـن کد نیز کامل است.

این دو کد ماندهٔ درجهٔ دوم تنها کدهای کامل (اعم از خطی و غیرخطی) با $n>d>۳$ اند. این کدها تاریخچهٔ جالبی دارنـد، هر دو کد در ۱۹۴۹ توسط گولی[1] [۸] کشف شده‌اند. او نخست با بررسی مثلث پاسکال ضرایب دوجمله‌ای (یا، درحالت کدهای سه‌سدای، شکل اصلاح شده‌ای از آن) امکان وجود چنین کدهایی را بررسی وماتریس آزمون زوجیت آنها را ارائه کرد، بدون آنکه تـوضیحی در مورد روش به‌دست آوردن این ماتریسها بدهد. همان‌طور که پیش از این نیز گفتیم، تنها کدهای کامل دیگر ، کدهای غیرخطی با $d=۳$ و با طول و اندازهٔ کدهای همینگ‌اند. دربخشهای بعد به‌کدهای گولی تعمیم یافته، که‌ساختار ترکیبیاتی جالب توجهی‌دارند، می‌پردازیم. ردهٔ تمام کدهای‌ماندهٔ درجهٔ دوم به‌طور گسترده‌ای مورد مطالعه قرارگرفته است، وکرانهایی برای فاصلهٔ مینیمم و برخی از مشخصات گروه خودریختیهای آن معلوم شده است. اما، برای اهداف ما اطلاعات فوق کفایت می‌کند.

شمارش وزن کدها

به‌طور شهـودی، ساختار فـاصله‌ای کد، کیفیت و بنابراین کارآیـی آن را تعیین می‌کـند. با دانستن آن می‌توان پارامترهایی نظیر احتمال خطارا، هنگامی‌که از کد در یك کانال گسسته استفاده می‌شود، محاسبه‌کرد. در حالت کلی توصیف کامل ساختار فـاصله‌ای بسیار پیچیده است، بنابراین به‌مسئله‌ای ساده‌تر می‌پردازیم ، یعنی تعیین تعداد کد واژه‌هایی‌که فاصله‌شان از یك کدواژهٔ مفروض $x\in C$ برابر i است، که این تعدادرا با $A_i(x)$ نشان‌می‌دهیم. واضح است که $A_i(\circ)$ همان تعداد کدواژه‌های به‌وزن i است. با اضافه‌کردن کدواژه‌ای چون y به‌هر کدواژه، کدبدون تغییر باقی‌می‌ماندو از اینجا نتیجه‌می‌گیریم که $A_i(y)=A_i(\circ)=A_i$ به‌عبارت دیگر، اگر تصورکنیم‌که روی یك‌کد واژه ایستاده‌ایم و به‌کد واژه‌هایی‌که دراطرافمان‌قرار دارند نگاه کنیم ، منظرهٔ مشاهده شده برای کلیهٔ کدواژه‌ها یکسان خواهد بود. **شمارندهٔ‌وزن** یك‌کد خطی (n,k) را باچند جمله‌ای دومتغیرهٔ

$$A(x,y)=\sum_{i=\circ}^{n}A_i x^i y^{n-i},\quad A_\circ=۱,\quad \sum_{i=۱}^{n}A_i=q^k-۱$$

تعریف می‌کنیم، که بازهم A_i تعداد کد واژه‌های به‌وزن i، یا تعداد کـد واژه‌هایی است‌که فاصله‌شان ازیك‌کد واژهٔ مفروض i است. شمارنده وزن‌کد را به‌طور یکتا تعریف نمی‌کند زیرا دوکد متفاوت می‌توانند شمارندهٔ وزن یکسانی‌داشته باشند. با وجود این‌شمارندهٔ وزن توصیف‌کنندهٔ مناسب ومفیدی برای یك‌کد است.

به‌عنوان مثالهایی ازشمارنده‌های وزن، کدهایی‌را که قبلا بررسی کـرده‌ایم. در نظر می‌گیریم. شمارندهٔ وزن‌کد $(۷,۴)$همینگ بافاصلهٔ ۳، عبارت است از

---

1. Golay

$$h(x,y)=x^{7}+7x^{4}y^{3}+7x^{3}y^{4}+y^{7}$$

وشمارنده وزن توسیع (۸,۴) این‌کد عبارت است از

$$H(x,y)=x^{8}+14x^{4}y^{4}+y^{8}$$

کد دودویی دوری (۲۳,۱۲) گولی با فاصلهٔ مینیمم ۷، دارای شمارندهٔ وزن

$$g(x,y)=x^{23}+253x^{16}y^{7}+506x^{15}y^{8}+1288x^{12}y^{11}+1288x^{11}y^{12}$$
$$+506x^{8}y^{15}+253x^{7}y^{16}+y^{23}$$

است، ونیز توسیع (۲۴,۱۲) این‌کد شمارهٔ وزنی برابر با

$$G(x,y)=x^{24}+759x^{16}y^{8}+2576x^{12}y^{12}+759x^{8}y^{16}+y^{24}$$

دارد. توجه کنید که شمارنده‌های وزن کدهای توسعه یافته (۸,۴) و (۲۴,۱۲) ایجاب می‌کنند که این کدها دوگان خودشان باشند.

یکی ازقضایای بنیادی نظریهٔ کدگذاری، منسوب به ف. ج. مك‌ویلیامز[1]، شمارندهٔ وزن یك کد (n,k) خطی‌را به‌شمارندهٔ وزن دوگانش مربوط‌می‌کند. مشخصاً اگر $A(x,y)$ شمارندهٔ وزن C و $A'(x,y)=\sum_{i=0}^{n}A'_i x^i y^{n-i}$ شمارندهٔ وزن C' باشد، آنگاه اتحادهای مك‌ویلیامز بیان می‌دارد که

$$A(x,y)=\left(\frac{1}{q^{n-k}}\right)A'(y-x,y+(q-1)x) \qquad (2)$$

از بسط چند جمله‌ایها ومقایسه ضرایب، شکل معادلی از این‌رابطهٔ چند جمله‌ای حاصل‌می‌شود که عبارت است از

$$\sum_{i=0}^{n-j}\binom{n-i}{j}A_i=q^{k-j}\sum_{i=0}^{j}\binom{n-i}{n-j}A'_i \qquad j=0,1,\cdots,n$$

ماتریس $\lambda=(\lambda_{ij})$ را که $\lambda_{ij}=\binom{n-i}{j}$، $0\leqslant i,j\leqslant n$، درنظر می‌گیریم. به سادگی و با استفاده‌از دنباله‌ای از اعمال سطری‌مقدماتی‌می‌توان‌این ماتریس را به‌یك‌ماتریس‌واندرموند تحویل کرد، ولذا این‌ماتریس‌نامنفرد است. این‌واقعیت که شمارندهٔ وزن یك کد، شمارندهٔ وزن دوگانش را به‌طوریکتا تعیین می‌کند، اغلب مفید واقع می‌شود.

یك نتیجهٔ مهم وفی‌البداهٔ اتحادهای مك‌ویلیامز که برای مقاصدمان به‌آن نیازداریم از این قرار است. اگر d' فاصلهٔ مینیمم C' باشد، آنگاه

1. F. J. MacWilliams

$$\sum_{i=0}^{n-j}\binom{n-i}{j} A_i=q^{k-j}\binom{n}{n-j} \qquad j=0,1,\ldots,d'-1 \qquad (۳)$$

زیرا $A'_0=1$، وبه‌ازای $1\leqslant i\leqslant d'-1$، $A'_i=0$. اگر کد C تنها s وزن ناصفر داشته باشد و $s\leqslant d'$، آنگاه دستگاه d' معادله و s مجهول فوق جوابی یکتا دارد.

به‌عنوان مثالی از این‌وضعیت، فرض‌کنید C یك‌کد (n,k) بهینه روی F_q باشد، یعنی فاصلهٔ مینیمم d آن، برابر $n-k+1$ باشد، و فرض‌کنید G و H به‌ترتیب ماتریس مولد وماتریس آزمون زوجیت آن‌باشند. حال هرمجموعه از k ستون G باید مستقل خطی‌باشند، زیرا در غیر این صورت‌کد واژهٔ ناصفری وجود خواهد داشت‌که در این k مختص برابر صفر است وبنابراین‌کد واژه‌ای باوزن نابیشتر از $n-k$ به‌دست می‌آیدکه با این‌واقعیت کــه فاصلهٔ مینیمم کد $n-k+1$ است، تناقض دارد. بنابراین فاصلهٔ مینیمم C'، که یك کد $(n,n-k)$ است، دست‌کم برابر $k+1$ است و در نتیجه C' نیز بهینه خواهد بود. به‌ازای $d'=k+1$، معادلات(۳)دستگاهی‌از kمعادله برحسب‌مجهولهای A_d، A_{d+1}،...، A_n تشکیل می‌دهند واز آنجاکه $d=n-k+1$، معادلاتی برحسب k مجهول داریم‌که‌می‌توان آنها را به‌طور یکتا حل‌کرد. اگر C یك‌کد بهینهٔ (n,k) روی F_q باشد، محاسباتی نه‌چندان مشکل نشان می‌دهدکه

$$A_{n-1}=\sum_{r=i}^{k-1}(-1)^{r-i}\binom{r}{i}\binom{n}{r}(q^{k-r}-1) \qquad i=0,1,\ldots,k-1 \qquad (۴)$$

مثال ساده‌ای [۹] ازیك کد بهینه روی F_3 عبارت است ازکد (۴,۲) همینگ، که فاصله‌اش۳، و ماتریس مولدش

$$G=\begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{bmatrix}$$

است، و با تــولید فضای سطری G می‌تــوان مستقیمــاً تحقیق کــردکه شمارنــدهٔ وزن آن $A(x,y)=8xy^3+y^4$ است.

حالتی‌که‌کد دوگان خودش باشد، یعنی $C=C'$، ازدیدگاه ترکیبیاتی بسیار جالـب توجه است. دریك کد دو دویی خوددوگان باید وزن همهٔ کد واژه‌ها بر ۲ بخشپذیر باشد. اما همان‌گونه‌که‌کدهای‌تعمیم یافتهٔ (۸,۴) همینگ و (۲۴,۱۲) گولی نشان می‌دهند، ممکن است‌که وزن هر کد واژه بر ۴ بخش‌پذیر باشد. نتیجهٔ جالبی منسوب بـه گلیسن[1] وپیرس[2] [۱۰] می‌گویدکه اگر C یك‌کد خود دوگان روی F_q باشدکه برای آن وزن هرکـد واژه بر c بخشپذیر باشد، آنگاه تنها چهارحالت برای (q,c) امکان‌پـذیر است‌کـه عبارتند از (۲,۲)،(۲,۴)، (۳,۳)و(۴,۲). این‌نتیجه‌ای بسیارعمیق است، واثباتش‌نیازمندابزارهایی اساسی‌خواهد بود.

---

1. Gleason 2. Pierce

این شرط که یک کد خود دوگان باشد، محدودیت شدیدی در مورد شکلی که شمارندهٔ وزن آن‌می‌تواند داشته باشد اعمال می‌کند. در اینجا تنهاحالت دودویی را بررسی‌می‌کنیم. از (۲) دیده می‌شود که اگر $A(x,y)$ شمارندهٔ وزن یک‌کد خوددوگان $(n,n/۲)$ (nزوج است) باشد، آنگاه

$$A(x,y)=\frac{۱}{۲^{n/۲}}A(y-x,y+x)=A\left(\frac{y-x}{\sqrt{۲}}\text{ و }\frac{y+x}{\sqrt{۲}}\right)$$

بدعلاوه، چون تنها وزنهای زوج می‌توانند درکد ظاهر شوند، $A(x,y)=A(x,-y)$. پس $A(x,y)$ تحت اثر تبدیلات

$$\frac{۱}{\sqrt{۲}}\begin{bmatrix}-۱ & ۱\\ ۱ & ۱\end{bmatrix}\text{ و }\begin{bmatrix}۱ & ۰\\ ۰ & -۱\end{bmatrix}$$

وبنابراین تحت اثر گروه ماتریسهایی که توسط این دو ماتریس پدید می‌آید، یعنی گروه دووجهی مرتبهٔ ۱۶، پایاست [۹]. با استفاده از نظریهٔ پایاها برای این گونه چندجمله‌ایها می‌توان نشان داد که اگر C یک کد دودویی خوددوگان به‌طول n باشد، شمارندهٔ وزن آن مجموعی خطی از حاصلضرب چند جمله‌ایهای $f(x,y)=x^۲+y^۲$ و $H(x,y)=x^۸+۱۴x^۴y^۴+y^۸$ (شمارندهٔ وزن‌کد تعمیم یافتهٔ همینگ)است. به‌عبارت دیگر

$$A(x,y)=\sum_{۲r+۸s=n}a_{rs}\,f(x,y)^r\,H(x,y)^s$$

اگر این محدودیت اضافی را نیز اعمال کنیم که وزن هرکد واژه بر۴ بخش‌پذیر باشد، آنگاه

$$A(x,y)=\sum_{۸r+۲۴s=n}a_{rs}H(x,y)^rG(x,y)^s$$

که در آن $G(x,y)$ شمارندهٔ وزن‌کد تعمیم یافتهٔ‌گولی است. دراین حالت طول‌کد همواره بر ۸ بخش‌پذیر است. برای‌دوحالت دیگر، یعنی $q=۳$ که‌همهٔ وزنها بر ۳ بخش‌پذیرند و $q=۴$ که همهٔ وزنها بر ۲ بخش‌پذیرند، نیز نتایج مشابهی برقرار است.

طرحهای ترکیباتی

مبحث طرحهای ترکیباتی موضوعی‌نسبتاً جامع است . در واقع من قصد دارم تنها دوتا از این طرحها، یعنی آرایه[1]های متعامد و tـ طرحها را شرح دهم. این امر بدین معنی نیست‌که دیگراشیای ترکیباتی‌ازقبیل‌صفحه‌های‌افکنشی[2]، هندسه‌های‌اقلیدسی‌وافکنشی، مربعهای‌لاتین، وماتریسهای آدامار[3] وغیره در نظریهٔ‌کدگذاری بی‌اهمیت وارزش‌اند، بلکه تنها به‌این‌معنی

---

1. array　　2. projective planes　　3. Hadamard

است‌که در این مقاله ترجیح داده‌ام توجه خود را به‌این دوطرح معطوف کنم.

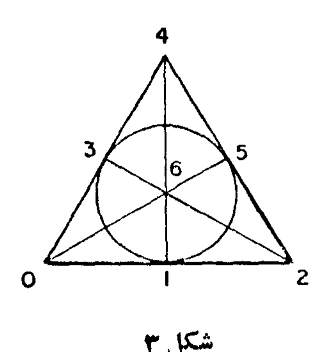
یك آرایهٔ متعامد (M,n,q,r,μ) عبارت‌است از یك آرایهٔ $M\times n$ روی الفبایی با q نماد، به‌قسمی‌که هر r ستون آن هر یك از q^r ـr تایی ممکن را دقیقاً μ بار دربرداشته باشد. پارامتر r توان آرایه و μ شاخص آن‌نامیده می‌شود؛ البته واضح است که $M=\mu q^r$.

مثالی ازیك آرایهٔ متعامد عبارت است ازکدسه‌سه‌ای (۴,۲) که پیشتر آن‌را بررسی کردیم (در واقع این‌کد، یك‌کد همینگ روی F_3 است):

۰	۰	۰	۰
۰	۱	۱	۱
۱	۲	۱	۰
۰	۲	۲	۲
۲	۱	۲	۰
۱	۰	۲	۱
۲	۲	۰	۱
۱	۱	۰	۲
۲	۰	۱	۲

این کدمثالی از یك‌آرایهٔ متعامد(۹,۴,۳,۲,۱) است، زیرا هردوتا ازستونهایش راکه‌درنظر بگیریم، هرزوج‌مرتب ازعناصر F_3 را دقیقاً یك‌بار دربردارد. این آرایه‌ها به‌طورگسترده‌ای بررسی شده‌اند، اما ازآنجا که تنها به‌ارتباطشان باکدها علاقه‌مندیم، شرح بیشتر آنها راتا بخش بعد به‌تعویق می‌اندازیم.

شیء ترکیبیاتی دیگری‌که موردتوجه ماست، tـ طرح است. یك t-(v,k,λ) **طرح**-t عبارت است ازگردایه‌ای اززیر مجموعه‌های kـتایی (که معمولا بلوك نامیده می‌شوند)یك مجموعهٔ v عنصری V به قسمی که هر زیر مجموعهٔ tـتایی از V دقیقاً در λ بلوك ظاهر شود. یك ۲ـ طرح‌معمولا یك**طرح بلوکی غیرکامل متعادل** نامیده می‌شود . یك tـ طرح با $\lambda=1$



شکل ۳

یك **دستگاه‌اشتاینر**[1] وچنانچه $k=3$ و $\lambda=1$ یك **دستگاه سه‌تایی‌اشتاینر** نامیده می‌شود.[2]
هندسهٔ فانو[3] که‌درشکل ۳ نشان‌داده شده است، مثال ساده‌ای از یك ۲- طرح است. دراین‌طرح مجموعهٔ V عبارت است‌از $\{0, 1, ..., 6\}$، وهر بلوك ازنقاط روی‌یك‌خط تشکیل شده‌است، دایره نیزیك خط به‌شمار می‌آید. بلوکها عبارت‌اند از $\{1,3,5\}$ ، $\{0,3,4\}$ ، $\{0,1,2\}$ ، $\{0,5,6\}$ ، $\{1,4,6\}$ ، $\{2,3,6\}$ و $\{2,4,5\}$ ، و هر زیر مجموعهٔ ۲-تایی دقیقاً دریك بلوك قرار می‌گیرد. برای مراجعات بعدی، توجه می‌کنیم‌که هربلوك دستگاه را می‌توان بایك هفتگانهٔ دودویی نمایش‌دادکه مختصات آن باعناصر V برچسب خورده است ودرنقاط بلوك برابر ۱ ودرسایرجاها صفراست. هندسهٔ فانو تناظرزیر رابه‌دست می‌دهد:

$\{1,3,5\}$	۰۱۰۱۰۱۰	$\{1,4,6\}$	۰۱۰۰۱۰۱
$\{0,3,4\}$	۱۰۰۱۱۰۰	$\{2,3,6\}$	۰۰۱۱۰۰۱
$\{0,1,2\}$	۱۱۱۰۰۰۰	$\{2,4,5\}$	۰۰۱۰۱۱۰
$\{0,5,6\}$	۱۰۰۰۰۱۱		

توجه کنیدکه این‌هفتگانه‌ها دقیقاً کدواژه‌های به‌وزن ۳ درکد $(7,4)$ همینگ‌اند،که‌پیش‌از این بررسی‌کردیم.

بسیاری از مطالب بخش‌بعد پیرامون خواص t- طرحها هستند، بنابراین بهتر است‌که این‌خواص رادراینجا شرح‌دهیم. بنا به‌تعریف، تعداد بلوکهایی از یك t-(v,k,λ) طرح‌که یك t- تایی مفروض را دربردارند برابر λ است. محاسبهٔ ساده‌ای نشان می‌دهدکه اگر λ_i تعدادبلوکهایی باشدکه یك‌زیرمجموعهٔ i-تایی مفروض را دربردارند، آنگاه

$$\lambda_i=\frac{\lambda\binom{v-i}{t-i}}{\binom{k-i}{t-i}} \quad i=0,1,\dots,t$$

که $\lambda=\lambda_t$ و λ_0 تعداد بلوکهای طرح است.

بحث شمارشی‌زیرکه در [۱۱] آمده‌است وعملا تعمیمی‌ازبحث ارائه‌شده‌در [۱۲] است، اطلاعات ساختاری مفیدی درمورد یك t-طرح فراهم می‌کند. فرض‌کنید S یك زیر-مجموعهٔ s- تایی دلخواه از V، و $y_i(S)$ تعداد بلوکهایی از t- طرح باشد که S را در دقیقاً i عضوقطع می‌کنند. تعداددفعاتی راکه‌یك r- تایی درمقطع S ویك‌بلوك ظاهرمی‌شود، به‌دوطریق می‌شماریم. S شامل $\binom{s}{r}$ r- تایی است وهریك‌ازاینهادر λ_r بلوك ظاهرمی‌شود. ازطرف دیگر، اگر I مجموعه‌ای i- تایی ومقطع S ویك‌بلوك باشد، آنگاه I تعداد $\binom{i}{r}$

---

1. Steiner

۲. برای‌یك‌دستگاه‌سه‌تایی اشتاینر معمولاعلاوه‌برشرایط بالا،شرط $t=2$ رادرنظرمی‌گیرند.-م.

3. Fano

r- تایی در مقطع S و یك بلوك فراهم می‌آورد. به‌این ترتیب $\binom{i}{r}y_i(S)$ تا از این r-تایی‌ها به‌دست می‌آید. بنابراین،

$$\sum_{i=r}^{s}\binom{i}{r}y_i(S)=\binom{s}{r}\lambda_r \;,\quad r=0,1,\ldots,\min(s,t) \qquad (۵)$$

این دستگاهی با $\min(s,t)+1$ معادله و $(s+1)$ مجهول است، و چنانچه $s\leqslant t$، این دستگاه جواب یکتایی خواهد داشت که مستقل از S است:

$$y_l(S)=y_l=(-1)^l\sum_{r=0}^{s}(-1)^r\binom{r}{l}\binom{s}{r}\lambda_r,\quad l=0,1,\ldots,s \qquad (۶)$$

اگر $s>t$، معادلات (۵) درحالت کلی جواب یکتایی ندارند، اما درحالت خاصی که $s=t+1$، می‌توانیم معادلهٔ r ام رادر $(-1)^r$ ضرب کنیم وسپس با جمع‌بندی روی r به معادلهٔ زیر برسیم:

$$y_0(S)+(-1)^t y_{t+1}(S)=\sum_{r=0}^{t}(-1)^r\binom{t+1}{r}\lambda_r \qquad (۷)$$

چون طرف‌راست این معادله مستقل‌از S است، نتیجه می‌گیریم که‌سمت چپ نیز چنین‌است.

نخستین کاربرد این روابط، ساختن‌طرحهای جدید از یك‌طرح مفروض‌است. مجموعهٔ تمام بلوکهای یك t-(v,k,λ) را با $\mathcal{B}$ ومکملهای این بلوکها را با $\mathcal{B}'$ نمایش می‌دهیم، یعنی، $\mathcal{B}'=\{(V\setminus B):B\in\mathcal{B}\}$. ادعا می‌کنیم که $\mathcal{B}'$ یك‌t- طرح است. برای اثبات، باید نشان‌دهیم که تعداد بلوکهایی که یك t- تایی را در بردارند، عددی است ثابت که از انتخاب t- تایی مستقل است. اما این عدد دقیقاً تعداد بلوکهایی از $\mathcal{B}$ است که بااین t- تایی مفروض هیچ اشتراکی‌ندارند؛ حال معادلهٔ (۶) با $l=0$ و $s=t$ نشان‌می‌دهدکه این عددبرابر y_0 است و به واقع‌از t- تایی انتخاب شده مستقل است. درنتیجه‌بلوکهای $\mathcal{B}'$ یك t-$(v,v-k,y_0)$ t-طرح تشکیل می‌دهند.

به‌عنوان مثالی‌ازمکمل یك‌طرح، مکمل طرحی راکه ازهندسهٔ فانو به‌دست‌آمد، درنظر بگیرید. بلوکهای آن‌عبارت‌انداز $\{۶,۴,۲,۰\}$،$\{۶,۵,۲,۱\}$، $\{۶,۵,۴,۳\}$، $\{۴,۳,۲,۱\}$، $\{۵,۳,۲,۰\}$، $\{۵,۴,۱,۰\}$ و $\{۶,۳,۱,۰\}$. چون کد(۷,۴) همینگ برداری را که همهٔ درایه‌هایش ۱اندربردارد، مکمل‌کدواژه‌هایی به وزن ۳، کدواژه‌هایی به وزن ۴ اند، و اینها نیز با بلوکهای فوق متناظرند. طرح فوق یك (۲,۴,۷)-۲ ۲-طرح است.

دربخش‌قبل دیدیم که چگونه‌می‌توان یك‌کدرا باروشی طبیعی‌و باافزودن یك‌رقم آزمون زوجیت توسعه‌داد. تحت‌شرایط معینی می‌توان‌یك t-طرح رانیز توسعه داد، ودراین حالت، این‌دوعامل توسعه نظیر هم‌اند. فرض می‌کنیم t عددی زوج و $(V,\mathcal{B})$ یكt-$(2k+1,k,\lambda)$ طرح‌است. حال باافزودن نماد ∞ به V مجموعهٔ $V'=V\cup\{\infty\}$ راتشکیل می‌دهیم، هر

گاه مجموعهٔ مکملهای بلوکهــای $\mathcal{B}$ در V را با $\overline{\mathcal{B}}$ و مجموعهٔ $\{B\cup\{\infty\}|B\in\mathcal{B}\}$ را با $\mathcal{B}'$ نمایش‌دهیم، ادعامی‌کنیم که‌مجموعهٔ بلوکهای $\overline{\mathcal{B}}\cup\mathcal{B}'$ یك $(t+1)$-$(2k+2, k+1, \lambda)$ طرح است. اثبات سرراست‌است. یك‌زیرمجموعهٔ $(t+1)$ ـ تایی T رادرنظر بگیرید. اگر T شامل ∞ باشد، درهیچ یك‌از بلوکهای $\overline{\mathcal{B}}$ ظاهر نمی‌شود و دقیقاً در λ بلوك از $\mathcal{B}'$ ظاهر می‌شود، بنا بر این T در دقیقاً λ بلوك از $\overline{\mathcal{B}}\cup\mathcal{B}'$ ظاهر می‌شود. اگر T شامل ∞ نباشد، در دقیقاً $y_\circ(T)$ بلوك‌از $\overline{\mathcal{B}}$ و $y_{t+1}(T)$ بلوك از $\mathcal{B}'$ ظاهر می‌شود وبنا بر معادلهٔ (۷)، و با توجه به‌اینکه t زوج است، نتیجه می‌شود که

$$y_\circ+y_{t+1}=\sum_{r=\circ}^{t}(-1)^r\binom{t+1}{r}\frac{\lambda\binom{2k+1-r}{t-r}}{\binom{k-r}{t-r}}$$

$$=\frac{\lambda}{\binom{2k+1-t}{k-t}}\sum_{r=1}^{t}(-1)^r\binom{t+1}{r}\binom{2k+1-r}{k-r}=\lambda$$

درنتیجه $\overline{\mathcal{B}}\cup\mathcal{B}'$ یك $(t+1)$-$(2k+2, k+1, \lambda)$ طرح روی V' است.

ما برخی‌ازخواص tـ طرحها را بررسی کرده‌ایم، وبرای‌شرح این‌خواص ازکدها کمك گرفته‌ایم. حال، موقعیت بسیار کلیتری را درنظر می‌گیریم، ودربخش بعد قضایای آسموس‌ـ ماتسون رامی‌آوریم که پایهٔ آنچه درمورد ارتباط بین کدها وطرحها می‌دانیم به‌شمارمی‌آید.

قضایای آسموس‌ـماتسون

به‌طورشهودی، می‌توان حدس‌زدکه یك‌کد "خوب"، یعنی کدی‌که "به‌طورچگال مرتب شده باشد"، بایدساختار پیچیده‌ای‌داشته‌باشد، واین‌مطلب برای‌کدهای باطول کم‌درست به‌نظر می‌رسد. شاید بارزترین مثالها ازاین دست، کدهای‌کامل باشندکه در آنها کره‌های به‌شعاع e تمام F_q^n رامی‌پوشانندودرعین‌حال یکدیگر راقطع نمی‌کنند. حال‌نشان می‌دهیم که درواقع ازاین کدها می‌توان tـ طرح‌ساخت ومثالهای بخشهای‌قبل‌حالتهایی استثنایی نبودند. ارتباط‌نسبتاً ساده‌ای میان آرایه‌های متعامد وکدها وجوددارد، که پیش‌ازپرداختن به‌حالت جالبتر tـطرحها، این ارتباط‌رانشان‌می‌دهیم. همهٔ‌قضایا وبرهانهای‌این‌بخش، به‌استثنای‌پاراگراف‌آخر، به‌آسموس وماتسون منسوب‌اند. [۱۳ و ۱۴].

فرض‌کنید C یك‌کد (n,k) خطی‌و C' کد $(n,n-k)$ دوگان‌آن با فاصلهٔ مینیمم d' باشد. اگر G ماتریس‌مولدی برای C، ودرنتیجه یك‌ماتریس‌آزمون زوجیت برای C' باشد، از آنجاکه فاصلهٔ مینیمم C' برابر d' است، هرمجموعه از $d'-1$ ستون G مستقل خطی است. اگر D گردایه‌ای‌از $(d'-1)$ ستون G باشد، آنگاه بااعمال سطری مقدماتی روی G می‌توان ماتریس مولدجدیدی مانند G^* برای C ساخت‌که در $d'-1$ سطر نخست‌آن

و درمختصات متناظر D ماتریس همانی قرار گیرد. از این مطلب بلافاصله نتیجه می‌شود که در فضای سطری G^* روی F_q، و بنابراین در فضای سطری G، همهٔ $(d'-1)$گانه‌ها از عناصر F_q به تعدادی مساوی، یعنی $q^{k+1-d'}$ بار، ظاهر می‌شوند. پس هر کدخطی (n,k) روی F_q که فاصلهٔ مینیمم دوگانش d' باشد یك آرایهٔ متعامد $(q^k,n,q,d'-1,q^{k+1-d'})$ تشکیل می‌دهد. ملاحظات فوق، که بسیار ساده بدست آمد، عملا در نظریهٔ کدگذاری کارآیی بسیاری داشته است. (در بخش بعد تحت عنوان "مطالعات بیشتر" اشارات دیگری در این زمینه خواهیم داشت.)

حال به ارتباط میان کدها و طرحها بازمی‌گردیم. اگر وضعیت مختصات یك کد به طول n را با n عضو متمایز نشان دهیم، یك کدواژه بوزن w را می‌توان با مجموعهٔ وضعیت مختصات ناصفرش یکی گرفت؛ این مجموعه معمولا **محمل**[1] کد واژه نامیده می‌شود. عبارت "مجموعهٔ بردارهای بوزن w در یك کد، مؤید یك t- طرح است"، بدین معنی است که اگر محمل بردارهای بوزن w را به عنوان بلوکها در نظر بگیریم، مجموعهٔ بلوکهای متمایز یك t-طرح است. روی F_q هر مضرب اسکالر از یك کدواژه باز یك کدواژه است، و بنابراین هر محمل دست کم $(q-1)$ بار ظاهر می‌شود، اما برای تشکیل طرح تنها نماینده‌های متمایز را در نظر می‌گیریم. نخستین قضیه‌ای که از کدها طرح می‌سازد، بدیهی است ولی راه را برای قضایای بعدی می‌گشاید.

قضیهٔ ۱ [۱۴]. یك کدخطی (n,k) روی F_q بهینه است اگر و تنها اگر مجموعهٔ بردارهای با وزن مینیمم، مؤید یك طرح بدیهی باشد.

برهان. نخست فرض کنید که C یك کدخطی (n,k) با فاصلهٔ مینیمم d است و برای هر مجموعهٔ d-تایی از وضعیت مختصاتش کدواژه‌ای با این محمل وجود دارد. می‌خواهیم ثابت کنیم که C یك کد بهینه است، یعنی $d=n-k+1$. فرض کنید C_1 زیرکدی از C باشد که توسط بردارهای با وزن مینیمم پدید می‌آید و C'_1 دوگان آن باشد. از آنجا که فاصلهٔ C_1 برابر d است، هر مجموعه از $(d-1)$ ستون هر ماتریس مولد C'_1 مستقل خطی است و بعد $d-1$ دارد. بنابراین بعد C_1 برابر است با $n-(d-1)$ که کوچکتر یا مساوی k است: $n-d+1\leqslant k$. اما قبلا دیده‌ایم که $k\leqslant n-d+1$ و بنابراین $k=n-d+1$.

حال فرض کنید که کد خطی (n,k) و بهینهٔ C با فاصلهٔ مینیمم $d=n-k+1$ داده شده است. باید نشان دهیم که هر مجموعهٔ d-تایی از وضعیت مختصات آن، محمل یکی از کد واژه‌های دارای وزن مینیمم است. اما از معادلهٔ (۴) می‌دانیم که تعداد کد واژه‌های با وزن مینیمم برابر است با $A_{n-k+1}=A_d=\binom{n}{d}(q-1)$، وچون $\binom{n}{d}$ محمل ممکن وجود دارد، باید برای هر محمل ممکن یك کدواژه (و $(q-1)$ مضرب اسکالر آن) موجود باشد. زیرا، اگر دو کد واژه بوزن d محمل یکسانی داشته باشند و مضرب اسکالری از یکدیگر نباشند، درمیان ترکیبات خطی آنها باید کد واژه‌ای بوزن کمتر از d وجود داشته باشد، که یك تناقض است.

---

1. support

دوقضیهٔ بعد اندکی عمیقترند و به‌کدهای کامل وتوسیع آنها مربوط می‌شوند.

قضیهٔ ۲[۱۳]. یك‌کد خطی C با فاصلهٔ مینیمم $d=2l+1$ کامل است اگر و تنها اگر کد واژه‌های دارای وزن مینیمم، مؤید یك $(e+1)-(n,d,(q-1)^e)$ طرح باشند.

برهان. نخست فرض کنید که کد C کامل است، یعنی به‌ازای‌هر $x\in F_q^n$ کد واژهٔ یکتایی چون $c\in C$ وجود دارد به‌طوری‌که x درکرهٔ به‌شعاع e حول c قرارمی‌گیرد. به‌ازای‌هرمجموعهٔ $(l+1)$-تایی E از وضعیت مختصات، $(q-1)^e$ عنصر از F_q^n بـا محمل E وجود دارد هریك از این‌عناصر درگویی‌به‌شعاع e حول یکی ازکد واژه‌ها قرارمی‌گیرد، که این‌ایجاب می‌کندکه وزن آن‌کد واژه حداکثر برابر $d=2e+1$ و بنابراین $2e+1$ باشد.

پس‌کد واژه‌ها در $(e+1)$ مختص با E مشترك‌اند. به‌مانند بحث فوق، هردوکدواژه به‌وزن d باید مضرب اسکالری ازیکدیگر باشند. پس، با تقریب مضارب اسکالر، $(q-1)^e$ کد واژه وجود داردکه محملشان E را می‌پوشاند. چون‌این‌عدد به‌انتخاب E بستگی‌ندارد، این محملها یك‌طرح تشکیل می‌دهند.

حال فرض‌کنید محمل کد واژه‌های با وزن مینیمم یك $(e+1)-(n,d,(q-1)^e)$ طرح تشکیل‌دهند. می‌خواهیم‌نشان دهیم‌که هر $x\in F_q^n$ درفاصلهٔ e ازیك‌کد واژه قراردارد. فرض‌کنید x عنصری از F_q^n باکوچکترین وزن ممکن باشدکه درفاصلهٔ e ازهیچ‌کدواژه‌ای قرارندارد (وبنابراین $w(x)\geqslant e+1$، زیرا n-تایی صفر عضوی از C است). فرض‌کنید E یك مجموعهٔ $(e+1)$- تایی ازمختصات برگزیده از محمل x باشد. چون‌کد واژه‌های به وزن d یك $(e+1)$- طرح تشکیل می‌دهند، $(q-1)^e$ بلوك از طرح وجود داردکه E را دربرمی‌گیرد، وبادرنظرگرفتن مضارب اسکالر آنها $(q-1)^{e+1}$ کد واژه به‌وزن $2e+1$ وجود داردکه محمل آنها E را دربرمی‌گیرد. حال ازمیان این‌کد واژه‌ها دقیقاً یکی، مثلا C، وجود داردکه مقادیرش روی E همان مقادیر x است و بنابراین وزن $x-c$ حداکثر $w(x)-1$ خواهد بود. اما اگر x درفاصلهٔ دست‌کم $e+1$ ازهـرکد واژه باشد، $x-c$ نیزچنین است وبنابراین $x-c$ برداری به‌وزن حداکثر $w(x)-1$ است‌کـه فاصله‌اش از هرکد واژه دست‌کم $e+1$ است، که این با انتخاب x تناقض دارد و اثبات کامل است.

از به‌کاربستن این قضیه روی میدان F_2 دستگاههای اشتاینر حاصل مـی‌شود. دراین حالت می‌توانیم این‌قضیه را با اعمال محدودیتهایی برای‌کد تعمیم یافتهٔ C_e نیز بیان‌کنیم.

قضیهٔ ۳[۱۳]. فرض‌کنید C_e یك کـد خطی کامـل تعمیم یافته به‌طول $n+1$ و فـاصلهٔ $d+1=2e+2$ روی F_2 باشد. در این صورت مجموعهٔ بردارهای با وزن مینیمم، مؤید یك $(e+2)-((n+1),(d+1),1)$ طرح خواهد بود.

برهان. ازقضیهٔ ۲ می‌دانیم‌که بردارهای بـه‌وزن $2e+1$ در C یك دستگاه اشتاینر تشکیل می‌دهند. مختص اضافه شده را، که برای آزمون زوجیت است، با ∞ نشان دهید وفرض‌کنیدکه E یك مجموعهٔ $(e+2)$-تایی ازوضعیت مختصات باشد. اگر E شامل ∞ باشد، ازآنجاکه d فرد است، دقیقاً یك‌کد واژه‌به‌وزن d در Cموجود است که $E\setminus\{\infty\}$ را می‌پوشاند وبنابراین‌دقیقاً یکی‌ازواژه‌های C_e، E را می‌پوشاند. اگر E شامل ∞نباشد،

آنگاه E حداکثر در محمل یکی از کد واژه‌های به‌وزن d (یا معادلاً محمل برداری به‌وزن $d+1$ در C_e و شامل ∞) از C قرار می‌گیرد. اگر E در چنین محملی قرار نگیرد، ادعا می‌کنیم که باید در محمل برداری با وزن $d+1$ از C قرار داشته باشد. بردار دودویی به‌وزن $e+2$ که به E نظیر می‌شود در کره‌ای به‌شعاع e حول یك کد واژه قراردارد و بنا به‌فرض این کد واژه نمی‌تواند از وزن d باشد. از این‌مطلب بلافاصله نتیجه می‌شود که این بردار به‌وزن $2e+2$ است، یکتاست، و محمل آن E را می‌پوشاند.

قضیهٔ اخیر، عملا برای کدهای غیر خطی نیز به‌کار می‌رود. دراینجا t- طرحهایی را که از کدهای کاملی که پیشتر شرح دادیم به‌دست می‌آیند، به‌اختصار شرح می‌دهیم. کدهای همینگ روی F_q دارای پارامترهای $n=(q^m-1)/(q-1)$، $k=n-m$، $d=3$ هستند و بنا بر قضیهٔ ۲، ۲- طرحهای $((q-1),3,n)$-۲ به‌دست می‌دهند. بـه‌ازای $q=2$، این طرحها دستگاههای سه‌تایی اشتاینر ند؛ فاصلهٔ مینیمم کد تعمیم یافته ۴ است و کد واژه‌های به وزن ۴ یك $(1,4,1+n)$-۳ طرح تـولید می‌کنند، که یك دستگاه چهارتایـی اشتاینر نامیده می‌شود. کـد $(11,6)$ گولی روی F_3 دارای فاصله مینیمم ۵ است و بردارهای به وزن ۵ آن مؤید یك ۳-طرح $(4,5,11)$-۳ اند. درواقع این‌طرح عملا یك‌دستگاه‌اشتاینر $(1,5,11)$-۴ است، اما قضیهٔ فوق تا آن حد قوی نیست کـه مستقیماً این‌مطلب را نتیجه دهد. اگر این‌کد را با اضافه کردن یك مختص که مقدارش قرینهٔ مجموع دیگـر مختصات است توسعه دهیم، یك کد $(12,6)$ بافاصلهٔ مینیمم ۶ به‌دست می‌آید. کد واژه‌های به وزن ۶ یك دستگاه اشتاینر $(1,6,11)$-۵ تشکیل می‌دهند. کد $(23,12)$ دودویی گولی دارای فاصلهٔ مینیمم ۷ است و کد واژه‌های بـه‌وزن ۷ یك دستگاه اشتاینر $(1,7,23)$-۴ تشکیل می‌دهند. از توسعهٔ این کد یك کد $(24,12)$ بـا فـاصلهٔ مینیمم ۸ و یك دستگـاه اشتاینر $(1,8,24)$-۵ حاصل می‌شود.

دو ۵- طرح اشتاینری که از کدهای گولی به‌دست می‌آیند، تنها ۵- طرحهای اشتاینری هستند که تاکنون شناخته شده‌اند. به‌ازای λی بـزرگتر از یك ۵- طرحهای زیـاد دیگری شناخته شده‌اند، اما به‌ازای $t\geqslant 6$، تاکنون هیچ t-طرحی (خواه اشتاینر، وخواه‌غیراشتاینر) یافت نشده است.[1]

قضیهٔ زیر شاید منشاء بسیاری از کارهایی باشد که دراین‌مبحث انجام می‌شود. استدلال آن بسیار ساده، ولی نیرومند ومبتنی بر استفادهٔ هوشمندانه از اتحادهای مك‌ویلیامـز است. پیش از پرداختن به‌قضیه باید یك‌نکته را روشن‌کنم. درقضایای قبلی از این واقعیت‌استفاده شد که دو کد واژهٔ x و y به‌وزن d و بامحمل یکسان مضرب اسکالری ازیکدیگر نـد، زیرا درغیر این‌صورت می‌توان عنصری چون α از F_q یافت که $0<w(x-\alpha y)<d$، که با این واقعیت‌که d فاصلهٔ مینیمم کد است منافات دارد.

برای قضیهٔ بعد به‌تعمیمی از این خاصیت نیاز داریم. نخست ملاحظه کنید کـه اگر

---

۱. در ۱۹۸۶ ثابت شد که به ازای هر t، تعدادی نامتناهی t- طرح وجود دارد. ـم.

$w(x)=v$، آنگاه x دست‌کم $[v/(q-۱)]+۱$ درایهٔ ناصفر یکسان دارد. اگر x و y دوکد واژهٔ به‌وزن v و بامحمل یکسان ازیك‌کد خطی با فاصلهٔ مینیمم d باشند، عنصری چون α از F_q وجود داردکه $w(x-\alpha y)\leqslant v-\left(\left[\frac{v}{(q-۱)}\right]+۱\right)$. اگر عبارت سمت راست نامساوی از d کوچکتر باشد، x و y مضرب اسکالری از یکدیگر خواهند بود. در قضیهٔ آخر فرض براین است‌که C یك‌کد خطی (n,k) با فاصلهٔ مینیمم d، و فاصلهٔ مینیمم کد $(n,n-k)$ دوگان C' برابر e است. بزرگترین اعداد صحیحی را که درنامساویهای

$$w-\left(\left[\frac{w}{(q-۱)}\right]\right)<e \quad و \quad v-\left(\left[\frac{v}{(q-۱)}\right]+۱\right)<d$$

صدق‌می‌کنند به‌ترتیب با $v_\circ$ و $w_\circ$ نشان‌دهید. برای‌کدهای دودویی‌قراردهید $v_\circ=w_\circ=n$؛ نکتهٔ مهمی‌که باید به‌خاطر بسپاریم آن‌است‌که دوکد واژهٔ به‌وزن کوچکتر یامساوی $v_\circ$ وبا محمل‌یکسان مضرب اسکالری ازیکدیگرند. گزارهٔ مشابهی برای‌دوکد واژه به‌وزن‌کوچکتر یامساوی $w_\circ$ از C' نیز برقرار است.

قضیهٔ ۴ [۱۴]. فرض‌کنیدکه تعدادوزنهای ناصفری از C' که‌کوچکتر یامساوی $n-t$ اند، خود کوچکتر یا مساوی عدد مثبت $d-t$ باشد. در ایـن صورت ، برای هر وزن v ، که $s\leqslant v\leqslant v_\circ$ ، بردارهای به وزن v در C یك tـ طرح تشکیل می‌دهند، وبرای هروزن w ، $e\leqslant w\leqslant \min(n-t,w_\circ)$، بردارهای به‌وزن w در C' یك tـ طرح تشکیل خواهندداد.

برهان. اثبات حکم برای C' ازاثبات حکم‌برای C ساده‌تر است. لذا نخست به‌آن می‌پردازیم. برهانی‌که می‌آوریم نشان‌می‌دهد‌که مکمل‌محمل بردارهای به‌وزن w در C' ، وبنا براین خود محملها، یك tـ طرح تشکیل می‌دهند.

ساختن طرح‌از C'. فرض کنید T یك مجموعهٔ tـ تایی از مختصات و C^T کدی به طول $(n-t)$ باشدکه‌ازحذف مختصات T حاصل‌می‌شود. فرض‌کنید C'^{oaT} کدی باشدکه توسط بردارهایی از C'که درمختصات T صفرند، پدید می‌آید. حال C^T و C'^{oaT} متعامدند ویك‌کد$(n-t,n-t-k)$است. بنا به‌فرض $d<t$ واگر $x^T,y^T\in C^T$ یکسان‌باشند، آنگاه بردارهای نظیرآنها در C، یعنی y,x، فاصله‌ای حداکثربرابر $t-d$ خواهند داشت‌که‌یك تناقض است . بنابـراین $|C^T|=q^k$ ودوگان C^T همان C'^{oaT} است. حال فـرض کنید $W=\{w_۱,\dots,wd-t\}$ مجموعهٔ وزنهای‌ناصفر C'^{oaT} باشد و دقت کنید که وزن مینیمم C^T دست‌کم $d-۱$ است. ازبه‌کاربستن اتحادهای مك‌ویلیامز برای C و C'، معادلات

$$\sum_{j\in w}\binom{n-t-j}{\mu}A_j'^{aT}=q^{n-t-k-\mu}\binom{n-t}{\mu}-\binom{n-t}{\mu},\mu=\circ,۱,\dots,d-t-۱$$

به‌دست می‌آیدکه دستگاهی‌از $(d-t)$ معادله برحسب حداکثر $(d-t)$ مجهول‌است، ودر آن $A_j'^{oaT}$ تعدادکد واژه‌های به‌وزن j در C'^{oaT} است. ازاین معادلات جوابی یکتا برای توزیع‌وزنی C'^{oaT} به‌دست‌می‌آید، وبااستفاده ازاین توزیع، می‌توان توزیع وزنی C^T را

نیز به‌دست آورد و هردوی اینها از انتخاب T مستقل‌اند.

حال فرض کنید E_v مجموعهٔ محمل کد واژه‌های به وزن v در C' و $\overline{E}_v$ مجموعهٔ مکملهای این‌محملها باشد، که در آن $v \leqslant \min(w_c, n-t)$. تعداد مجموعه‌هایی از E_v که T را در بردارند دقیقاً $(q-1)/1$ برابر تعداد کدواژه‌های به‌وزن v در C'^{oaT}، و بنابراین از T مستقل است. پس مجموعه‌های $(n-v)$- تایی E_v یك t- طرح تشکیل می‌دهند. و در نتیجه بنابر خاصیتی که قبلا ثابت‌کردیم، مجموعه‌های v- تایی E_v نیز یك t- طرح تشکیل خواهندداد.

ساختن‌طرح‌از C. فرض‌کنید D_d مجموعهٔ‌محمل‌های‌کد واژه‌های‌به‌وزن d در C باشد. تعداد مجموعه‌های d- تایی D_d که‌یك t- تایی‌مفروض را دربردارند، $(q-1)/1$ برابر تعداد بردارهای به‌وزن $d-t$ در C^T است، و درنتیجه از انتخاب T مستقل است. پس مجموعه‌های d-تایی D_d یك t- طرح‌تشکیل‌می‌دهند. برای‌اثبات حکم درحالت $d<v\leqslant v_{\circ}$ از استقراء استفاده می‌کنیم، فرض‌کنید برای هروزن v، که $d<v<v'\leqslant v_{\circ}$ ، محمل کد واژه‌های به وزن v یك t- طرح تشکیل دهند. فرض کنید $D_{v'}$ مجموعهٔ کد واژه‌های به‌وزن v' باشد. تعدادزیرمجموعه‌هایی از $D_{v'}$ که T را دربردارند، $(q-1)/1$ برابر تعداد کد واژه‌های به‌وزن $v'-t$ در C^T است، که‌خود ازکدواژه‌های به‌وزن v در C' ناشی می‌شوند. تعدادکل کدواژه‌های به‌وزن $v'-T$ در C^T ازانتخاب T مستقل‌است. بنابه‌فرض همهٔ‌وزنهای کمتراز v' یك t- طرح فراهم می‌سازند. بنابراین تعداد بردارهایی به‌وزن $v'-t$ در C^T که‌ازکد واژه‌های به‌وزن‌کمتراز v' ناشی می‌شوند نیزازانتخاب T مستقل است. پس $D_{v'}$ یك t- طرح است.

روش اثبات این قضیه به‌ویژه جالب‌است. استفاده از اتحادهای مك‌ویلیامز وملاحظهٔ این‌که‌کدواژه‌های به‌وزن‌کمتراز $v_{\circ}$ وبامحمل یکسان، مضرب‌اسکالری ازیکدیگرند، پایه و اساس این برهان است.

• کاربردهای‌قضیه رابامثال بهتر می‌توان توضیح داد. جالبترین کاربرد آن در کدهای خوددوگانی است که در شمارندهٔ وزنشان شکافهایی وجود دارد. نخست مسئله را برای‌کد (۱۲,۶) گولی‌روی $F_۳$ حل می‌کنیم. این‌کد تنها کد واژه‌هایی به‌وزنهای ناصفر ۱۲,۹,۶ دارد؛ باانتخاب $t=$ ۵، تعدادوزنهای کوچکتر یامساوی $n-t=$ ۱۲ − ۵ برابر ۱ است که خودکوچکتر یامساوی است با $d-t=$ ۶ − ۵ = ۱. دراین‌حالت، کدواژه‌های به‌وزن ۶ مؤید یك‌دستگاه اشتاینر (۱,۶,۱۲)-۵، وکدواژه‌های به‌وزن ۹ مؤید یك‌طرح بدیهی‌اند که همهٔ زیرمجموعه‌های ۹ تایی روی ۱۲ عنصر را در بردارد. چنانچه این‌کد تعمیم یافته را به‌آن‌کدواژه‌هایی‌که دریك مختص خاص مقدارشان ۱ است محدودکنیم وبدانیم‌که این کد توسعه‌ای ازیك‌کد (۶,۱۱) است، قضیه نشان می‌دهد که‌کدواژه‌های به‌وزن ۵ درواقع یك ۴- طرح‌تشکیل می‌دهند، نتیجه‌ای‌که از قضیهٔ ۲ به‌سادگی حاصل‌نمی‌شد.

بررسی دوبارهٔ کددودویی (۱۲,۲۴) گولی‌نیز جالب‌است. دراین‌کدتنهاوزنهای ناصفر ۸,۱۲,۱۶,۲۴ است؛ باانتخاب $t=$ ۵ تعدادوزنهای‌کوچکتر یامساوی ۲۴ − ۵ خودکوچکتر یامساوی ۸ − ۵، یعنی ۳، است. پس محمل‌کدواژه‌های‌هروزن یك ۵- طرح تشکیل‌می‌دهند،

که این ۵-طرحها به‌ترتیب عبارتند از (۲۴,۸,۱)-۵،(۲۴,۱۲,۴۸)-۵،(۲۴,۱۶,۷۸)-۵ [۱۴]. به‌سادگی می‌توان نشان داد که این کد، کدواژه‌ای راکه همهٔ ارقامش یك است در بر دارد، وبنابراین مکمل کدواژهٔ به‌وزن ۸، کدواژهٔ به‌وزن ۱۶ خواهد بود وطرحهای متناظر مکمل یکدیگرند. طرحی که ازوزن ۱۲ به‌دست‌می‌آید، مکمل خوداست.

کدماندهٔ درجهٔدوم (۴۷,۲۴) روی F_2 ازفاصلهٔ مینیمم ۱۱ است وتوسیع آن تنها وزنهای ۱۲،۱۶،۲۰،۲۴،۲۸،۳۲،۳۶ و ۴۸ را دارد. ازاتحاد ملك‌ویلیامز نتیجه می‌شود که هر کد خودِ دوگان خطی با فاصلهٔ ۱۲ وطول ۴۸ که وزن هرکدواژه‌اش بر ۴ بخشپذیر باشد، شمارندهٔ وزن‌یکتایی دارد، که جزئیات آن دراینجا ذکر نمی‌شود. به‌ازای $t=5$، تعداد(۷) وزنهای ناصفر کوچکتر یامساوی $n-t=48-5$ برابر با $d-t=12-5$ است، وبنابر این کد واژه‌های نظیر هروزن مؤید یك ۵- طرح‌اند. پارامترهای آنها در [۱۴] آمده است ودراینجا تنها یادآوری می‌کنیم که چون این کد، کدواژه‌ای راکه همهٔ ارقامش یك‌است در بردارد، طرحهای به‌دست آمده‌از کدواژه‌های به‌وزن ۱۲،۱۶، و ۲۰ به‌ترتیب مکمل طرحهای به‌دست آمده ازوزنهای ۳۶، ۳۲ و ۲۸ اند، درحالی که طرح نظیر وزن۲۴، مکمل‌خوداست.

این بخش راباشرح خطوط کلی بحثی، منسوب به دلسارت[1] [۲۰] به‌پایان می‌بریم. وی تنها با بهره‌گیری ازاین فرض که C یك آرایهٔ متعامد است، نشان‌دادکه ازمیان محمل کد واژه‌های C می‌توان t- طرح ساخت. فرض کنید C یك کد خطی (n,k,d,q) با s وزن ناصفر، و C' دارای فاصلهٔ مینیمم d' و s' ناصفر باشد. فرض‌کنید $v\in F_q^n$ به وزن t، $t<d$، باشد و تعداد کدواژه‌هایی‌از C راکه دارای‌وزن τ هستند ودقیقاً در t مختص ناصفر u با آن‌مشترك‌اند، با $\lambda_\tau(u)$ نشان دهید. ازآنجاکه C یك آرایهٔ متعامد باتوان $d'-1$ است، می‌توانیم تعداد دفعات ظهور بردارهای به‌وزن $t+j$، $0\leqslant j\leqslant d'-1-t$ ، در C راکه با u دردقیقاً مختصات ناصفرمشترك‌اند، به‌دوطریق بشماریم:

$$\sum_{\tau}\binom{\tau-t}{j}\lambda_\tau(u)=\binom{n-t}{j}(q-1)^j q^{k-t-j}\quad j=0,1,\dots,d'-1-t$$

درسمت چپ جمع‌بندی روی s وزن ناصفر C انجام می‌شود. پس دستگاهی از m معادله و برحسب s مجهول $\lambda_\tau(u)$ حاصل‌می‌شود. اگر $s<d'$، می‌توانیم t را به‌صورت $d'-s$ تعریف‌کنیم وبه‌این ترتیب دستگاهی‌از s معادله‌و s مجهول‌حاصل می‌شود. ازآنجاکه‌ماتریس تبدیل نامنفرد است (دنبالهٔ ساده‌ای ازاعمال سطری مقدماتی این ماتریس را به‌یك ماتریس واندرموند تبدیل‌می‌کند) به‌ازای هر τ جواب‌یکتایی برای $\lambda_\tau(u)$ وجود دارد، واین نشان می‌دهدکه کد واژه‌های به‌هر وزن ناصفر C مؤید یك t- طرح‌اند، زیرا $\lambda_\tau(u)$ از انتخاب بردار u به‌وزن $d'-s$، مستقل‌است. مشابهاً در C' نیز کدواژه‌های به‌هر وزن ناصفر مؤید یك t- طرح‌انــد که در آن $t=\max(d'-\bar{s}',d'-\bar{s})$، و $\bar{s}$ برابـر $(\bar{s}-1)$ تعریف می‌شود هرگاه C کدواژهٔ متشکل‌ازارقام یك‌را دربرداشته باشد، ودرغیراین صورت برابر

1. Delsarte

s تعریف می‌شود. $\bar{s}'$ رانیز به‌طریق‌مشابهی‌تعریف می‌کنیم. این‌استدلال ساده، زیبا، ونیرومند است و به‌خوبی روابط جالبی راکه میان‌کدگذاری و ترکیبیات وجود دارد. نشان می‌دهد.

مطالعات بیشتر

آنچه دراین مقاله آمد، بیانگر کوششهایی است‌که تا سال ۱۹۷۲ صورت گرفته بود. از آن‌زمان این مباحث‌درد‌وجهت توسعه یافته‌اند،که درهردوی آنها مسائل جالبی مطرح شده است. جهت‌اول توسعه ازاین طرزفکر سرچشمه می‌گیردکه چون کدهای کامل در تولید t- طرحها مفیدبوده‌اند، شایدبتوان قیدکامل بودن یك‌کدرا به‌طریقی‌مهارشده اندکی ضعیفتر کرد بی‌آنکه دراین میان t- طرحهایی ازدست بروند. این اندیشه‌ای است که در ورای تعریف کدهای به‌طورریکنواخت چیده‌شده [۱۶،۱۷،۱۸، هرچند که دردوتای این مراجع تعاریف متفاوتی داده‌شده‌است] وکدهای تقریباً کامل نهفته‌است [۱۹]. این‌رهیافت واقعاً باموفقیتهایی نیز روبرو شده‌است.

جهت دیگر توسعه از کارهای بنیادی دلسارت [۳] ناشی می‌شود، که، یقیناً یکی از مهمترین‌کارهایی است‌که درچندسال‌اخیردرزمینهٔ کدگذاری انجام شده است. پیش‌از وی، کدهای غیرخطی‌وپیچیدهٔ متعددی شناخته‌شده بودندکه t- طرح به‌دست می‌دادند، امادرچارچوب هیچ یك ازنظریه‌های موجود درآن وقت نمی‌گنجیدند. کوششهایی درجهت تعریف دوگان یك‌کد غیرخطی صورت‌گرفته‌بود، اما به‌نظرنمی‌رسیدکه ازاین‌تعریف هم کاری ساخته باشد. دلسارت توزیع‌فاصله‌ای‌کدها را (به‌جای توزیع وزنی) درنظر گرفت وتبدیلی روی آن تعریف‌کرد. با این توزیع وتبدیل متناظرش، اوچهار پارامتر رامعرفی‌کرد. چنانچه‌کد خطی‌باشد، توزیع فاصله‌ای وتبدیلش، به‌توزیع‌وزنی ومضارب‌اسکالر توزیع وزنی‌کددوگان تحویل‌می‌شود. دراین‌حالت پارامترها عبارتنداز فاصلهٔ C یعنی d، تعداد وزنهای ناصفر C یعنی s، فاصلهٔ C' یعنی d'، وتعدادوزنهای ناصفردر C' یعنی s'. نتیجهٔ شگفت‌آوراین‌است که‌چنانچه برای کدهای غیرخطی‌این‌پارامترها رابه‌کاربریم، بسیاری‌ازنتایجی که برای‌کدهای خطی‌حاصل‌شد، هم‌ارزهای نیرومندی درموردکدهای غیرخطی‌دارند.

برای خوانندگانی‌که مایل‌اند این مبحث را دنبال‌کنند، مقالهٔ اصلی دلسارت [۲۰] خواندنی‌خواهد بود. کتاب مك‌ویلیامز واسلوان [۲۱] نیزشرح دقیقی‌ازبخش اعظم‌این کار رادربردارد. دومقالهٔ توصیفی‌آسموس وماتسون [۲] ووان‌لینت [۳] نیزجالب توجه‌اند. به غیرازاین مراجع، دیگرمقالات بیشتر به‌موضوعات خاص و حاشیه‌ای می‌پردازند وبرای مطالعات بیشترباید ازمراجع ذکرشده در [۲]،[۳]، یا [۲۱] کمك‌گرفت.

مراجع

1. Shanon, C. E., "A Mathematical Theory of Communication," *Bell System Tech. J.*, **27**(1948)379–423, 623–656.

2. Assmus, E.F.,Jr. and Mattson, H.F.Jr.,"Coding and Combinatorics," *SIAM Rev.*, **16**(1974)349-388.

3. Van Lint, J.H.,"Combinatorial Designs Constructed from or with Coding Theory,"in *Information Theory: New Trends and Open Problems* edited by G. longo, CISM Courses and Lectures 219, Springer-Verlag, Wien. 1975.

4. Hamming R.W., "Error Detecting and Error Correcting Codes," *Bell System Tech. J.*, **28**(1950)147—150

5. Tietavainen, A., "On the Nonexistence of Perfect Codes over Finite field," *SIAM J. Appl. Math.*, **24**(1973)88-96.

6. Tietavainen, A. and Perko, A., "There are no Unknown Perfect Binary Codes," *Ann. Univ , Turku., ser A*. **148**(1971)3-10.

7. Peterson, W.W. and Weldon, E.J.Jr., *Error-Correcting Codes*, MIT Press, Cambridge. 1972.

8. Golay. M.J.E., "Notes on Digital Coding,"*Proc.IRE.*,**37**(1949)657.

9. Sloane, N.J.A., "Weight Enumerators of Codes," *Mathematical Centre Tracts*,**55**(1974)111-138.

10. MacWilliams , F.J, Mallows, C.L. and Sloane, N.J.A., "Generalizations of Gleason's Theorem on Weight Enumerators of Self-Dual Codes,'*IEEE Trans. Information Theory*, **18** (1972) 794-805.

11. Alltop, W.O.,"Extending t-Designs,"*J. Combinatorial Theory*(A),**18** (1975)177—186.

12. Mendelsohn; N.S.,"Intersection Numbers of t-Designs," *Studies in Pure Mathematics*,Academic Press, New York,1971, 145-150

13. Assmus, E.F. and Mattson, H.F, "On Tactical Configurations and Error-Correcting Codes," *J. Combinatorial Theory*, **2**(1967)243-257.

14. Assmus, E.F. and Mattson, H.F. "New 5-Designs," *J. Combinatorial Theory*'**6**,(1969)122—151.

15. Goethals, J.M., "A Polynomial Approach to Linear Codes,"*Phillips Res. Repts.*,**24**(1969) 145—159.

16. Bassalygo, L.A., Zaitsev, G.V. and Zinovev, N.V., "Uniformly Packed Codes," *Problems of Information Transmission*,**10**(1974)6—10 (English Translation).

17. Goethals, J.M. and Van Tilborg, H.C.A,"Uniformly Packed Codes," *Phillip Res. Repts.*,**30**(1975)9-36

18. Semakov, N.V, Zinovev, V.A. and Zaitsev, "Uniformly Packed Codes," *Problems of Information Transmission*, **7** (1971) 30-39 (English Translation).
19. Goethals, J.M, and Snover, S.L., "Nearly Perfect Binary Codes, *Disc. Math*, **3** (1972) 65_68.
20. Delsarte, P., "Four Fundamental Parameters of a Code and their Combinatorial Significance", *Information and Control*, **23** (1973) 407-438.
21. MacWilliams, F.J. and Sloane, N.J.A., *The Theory of Error Correcting Codes*, North_Holland Publishing Co., Amsterdam, 1977.

